ABSTRACT OF THE DISCLOSURE

In general, data exchanged between users is protected using any of various encoding approaches. An example of encoding is encryption, but any kind of encoding may be used. The data used to encrypt the data exchanged between the users, referred to as a "key", is maintained only in a key repository. Users must obtain a key from the key repository to either encode or decode, encrypt or decrypt data, after which the user's copy of the key is destroyed or otherwise rendered inoperable. A key management policy is employed to control access to the keys maintained by the key repository. Encoding algorithms may be dynamically changed over time. Users may negotiate different algorithms to be used with specific users or messages. Thus, different algorithms may be used between different sets of users depending upon what the member users of those sets negotiate among themselves. The frequency at which algorithms are changed may also be separately negotiated between users. The frequency may vary depending, for example, upon the perceived risk of intrusion by unauthorized third parties, the content of the messages being transmitted, or both. According to an inline message decryption approach, an encoded message is provided to a user in a form that enables the user's client to process the encoded message using conventional client tools and obtain the cleartext message. This eliminates the need for a user's client to be aware of the particular encoding algorithm used to encode the message. Various embodiments of the inline message decryption approach include: a) in-situ decryption; b) remote decryption; and c) data uploading. An approach is also provided for exchanging data between nodes in a network using sets of associated URLs.